UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

1ST RATE MORTGAGE CORPORATION, et al.,

Plaintiffs,

v. Case No. 09-C-471

VISION MORTGAGE SERVICES CORPORATION, et al.,

Defendants.

DECISION AND ORDER

In this action Plaintiffs 1st Rate Mortgage Corporation and William Thayse, its owner, brought numerous claims against Defendant Vision Mortgage Services Corp. and several individuals who were former employees of 1st Rate. Plaintiffs allege that during 2008, Richard Robokoff, a part-owner and vice-president of 1st Rate, secretly formed a company (Vision) to compete with 1st Rate. While he was starting his own company, he negotiated a sale of his 1st Rate ownership interest to Thayse and signed a stock purchase agreement on April 11, 2008. Although he resigned from his position, he was to continue as an employee through the summer at a reduced salary. During this period, the complaint alleges that Robokoff orchestrated a conspiracy through which he and the other individual Defendants stole 1st Rate's confidential business information and other data, including client information and the employee handbook, by logging on to their company accounts and downloading information or emailing it to their personal computers. When 1st Rate discovered what was going on in May and June of 2008, it terminated the employees involved. It

alleges that by then it was too late, however, as Robokoff's new company had already started soliciting its customers and taking business away from 1st Rate.

In claims one, two and three, Plaintiffs allege that the activity described above violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. They also bring state law claims alleging breach of contract, breach of the duty of loyalty, civil conspiracy, tortious conversion, misappropriation of trade secrets, and fraud. The Defendants, in five separate motions, have moved for summary judgment on most of these claims. As set forth below, claims two, eight and ten will be dismissed, but the others will survive summary judgment.

I. CFAA Allegations

The Defendants argue that the CFAA allegations must be dismissed because the CFAA applies only when a computer or its data have been damaged. Here, all we have are alleged thefts or misappropriations of information the Defendants accessed through their own employee passwords. The information stolen was not destroyed but merely copied. The Defendants did not cause damage to the employer's computers, and the computer network's service was not disrupted in any way. The Defendants' reply brief appears to abandon this line of argument in favor of another, however, so I will address it with some brevity.

As noted above, the Defendants believe the CFAA requires a plaintiff to show that there has been some kind of damage to a computer system. Plaintiffs argue that the CFAA is not limited to instances in which a computer or network is actually damaged – it also allows recovery if the plaintiff has suffered a "loss." Section 1030(g) provides that "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain

compensatory damages and injunctive relief or other equitable relief." (emphasis added). The statute defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Using this definition, Plaintiffs allege they have been forced to incur "reasonable cost[s]" in "responding to an offense." *Id.* That is, even if their network or hard drive was not damaged and data was not erased, 1st Rate nevertheless had to respond to the theft of its information. For example, 1st Rate states that it spent several weeks checking the integrity of its computer system and data, and of course it needed to spend time figuring out which data had been compromised.

Plaintiffs are correct that the CFAA allows recovery for losses sustained even if data or computers were not damaged. In claim one, Plaintiffs are suing under § 1030(a)(4), which provides relief if a defendant "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. § 1030(a)(4). The private right of action is found in § 1030(g):

> Any person who suffers damage or loss by reason of a violation of this section [1030] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages . . . .

18 U.S.C. § 1030(g).

The factors set forth in § (c)(4)(A)(i) include: "(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value." Thus, reading all these subsections together, courts have concluded that there is a private right of action under § 1030(a)(4) so long as the conduct involves a loss of at least $5,000 in value. There does not, in other words, need to be "damage" independent of the loss; it is enough that the plaintiff suffer a loss that qualifies under the statute. *NCMIC Finance Corp. v. Artino,* 638 F. Supp. 2d 1042, 1063-1064 (S.D. Iowa 2009) ("Courts have interpreted 'loss' to include the cost of responding to a security breach, such as the cost of performing a computer system damage assessment, even if the losses are not derived from any change to the computers themselves or the information contained on the computer."); *see also Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro,* 2007 WL 1847435, *5 (M.D. Pa. 2007) ("while Defendants may be correct in arguing that [there was] no physical damage or impairment to the integrity of SPI's computer system, the CFAA has been held to apply in cases involving former employees wrongfully acquiring and using a plaintiff employer's confidential or trade secret information.") Even the case relied on by the Defendants held as much, and it called the argument now made by the Defendants "counterintuitive." *SKF USA, Inc. v. Bjerkness,* 636 F. Supp. 2d 696, 720 (N.D. Ill. 2009). As noted above, however, it appears from the reply brief that the Defendants have abandoned this argument, and so I will move on to the alternative argument they raise in their reply brief.

In their reply brief, Defendants focus on a different part of the statute. They note that the statute defines "loss" as "any reasonable cost to any victim," 18 U.S.C. § 1030(e)(11), and argue

that the costs cited by Plaintiffs were not *reasonably* incurred as responses to the breaches they allege occurred. After all, the Defendants were employees simply accessing information through the normal course of business and their company-issued passwords. Because the information theft was an "inside job," there would have been no reason to conduct a system-wide security check or spend money and resources on such matters because the activities the Defendants engaged in (copying, downloading, and emailing) did not cause any harm and would not require anything more than deleting the employees' accounts or changing passwords. The Defendants further argue that the losses incurred do not meet the $5,000 threshold required by the CFAA.

I first note that these arguments have been waived. *Graff v. City of Chicago,* 9 F.3d 1309, 1318 n. 6 (7th Cir.1993) (argument first raised in reply brief is waived). A litigant cannot move for summary judgment on one ground and then switch gears when its opponent presents a convincing opposition. This is especially true in the summary judgment context. Many district courts, including this one, do not routinely hear oral argument, which means the reply brief is the last word it will hear on the issue. Allowing the movant to present a novel argument in its reply brief would deny the other side any opportunity for rebuttal.

Even if I considered the waived arguments, however, I would conclude that at best they present jury questions. The "reasonableness" of a company's reaction to stolen data involves questions of judgment that invoke practical, rather than legal, concerns. (And a jury might well look askance when individuals who stole from a company protest that the victim of the theft overreacted.) Moreover, courts have noted that the CFAA has frequently been used to remedy "inside jobs" just like the one alleged here. *See, e.g., Pacific Aerospace & Electronics, Inc. v. Taylor,* 295 F. Supp.2d 1188, 1196 (E.D. Wash. 2003) (noting that while "the majority of CFAA

cases still involve 'classic' hacking activities[,] ... [e]mployers ... are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system.") Presumably in such employee theft cases the companies' security responses are similar to those at issue here, yet that does not seem to be a bar to relief. What matters is whether the employer's reaction was reasonable, not whether it was strictly necessary to continuing in business. The allegations contained in the complaint suggest a brazen (and successful) attempt to replicate an existing business by stealing information from it. A jury could well conclude that the actions 1st Rate Mortgage took upon discovering the theft were reasonable responses to the situation and that its response costs exceeded $5,000. Accordingly, I will decline to grant the Defendants' motion for summary judgment on claim one.

Claim two, however, relies on § 1030(a)(5). That subsection prohibits certain conduct, such as unauthorized access to a computer, but it also requires that "damage" occur. Because Plaintiffs have not alleged that their systems were damaged (and their briefs do not contest the point), claim two will be dismissed. Claim three, for conspiracy, may proceed because it depends on the conduct alleged in claim one.

II. Claims Particular to Defendant Robokoff

In claim four, Plaintiffs assert that Defendant Robokoff breached the stock purchase agreement he signed upon selling his interest in the company. In exchange for more than $200,000, Robokoff agreed to turn over to 1st Rate "constructive possession of all passbooks, keys, and other data of the Companies . . .[and] complete books and records relating to the business of the

Companies, to the extent any such items are within the control or knowledge of the Seller [i.e., Robokoff]." (Dkt. # 64 at Bates 000003[1].) Plaintiffs argue that Robokoff orchestrated a scheme by which he and the other Defendants removed and copied company records. As such, he had knowledge that these records existed, yet he kept them for himself and his new company rather than turning them over to 1st Rate.

Robokoff argues that the only thing he took was a copy of the company handbook, and he wonders how that would constitute a breach of any contractual duties. First, there is no *de minimis* clause in the stock purchase agreement: it requires the turning over of *complete* books and records, not just some or most. Second, the Plaintiffs are not concerned about the employee handbook. The contractual duty to turn over company records extends to those records within the control and knowledge of Robokoff, not just those he personally took home. If Plaintiffs' version of events is believed by a jury, clearly Robokoff had both knowledge of and control of the pertinent records because he was the prime mover in orchestrating their removal. Of course the entire point of such a contractual provision is to keep company records in the hands of the company itself so that competitors do not obtain competitive advantage. When an individual assists a competitor in

---

[1]Under Local Rules, proposed findings of fact must contain "specific references to the affidavits, declarations, parts of the record, and other supporting materials relied upon to support the fact described in that paragraph." Civil L. R. 56(b)(1)(C)(i). Typically a document like a contract would be filed as an attachment to an attorney's affidavit or declaration and then referred to as (for example) "Smith Aff., Ex. 3 at 5-6." To the extent the briefs and proposed findings contain any citations to the stock purchase agreement, they refer only to Bates stamp numbers, which do not correspond to anything docketed in the record. Thus, the local rules are designed to ensure ease of access by requiring that anyone wishing to view the cited document would know exactly where to look for it on the electronic docket.

I further note that the proposed findings and responses perpetuate an unfortunate but common practice of arguing points of law as well as the implications of such facts (e.g., "Agreed, but dispute that Smith was under a contractual obligation."). Proposed findings should be concise statements of *material* fact and in many cases could be limited to just a few pages.

obtaining the information – especially when the individual *is* the competitor – his claim that there can be no breach of contract claim will almost surely fail. Here, I conclude that a jury could find that Robokoff knew about and orchestrated the removal of several documents and files he was under a contractual duty to turn over.

In claim seven the Plaintiffs allege conversion based on Robokoff's taking of Plaintiffs' property. The elements of tortious conversion comprise: (1) intentionally controlling/taking property belonging to another; (2) controlling/taking property without the owner's consent; and (3) those acts resulting in serious interference with the rights of the owner to possess the property. *Bruner v. Heritage Companies,* 225 Wis. 2d 728, 736, 593 N.W.2d 814, 818 (Wis. Ct. App. 1999). Plaintiffs allege that Robokoff intentionally controlled the property of 1st Rate by orchestrating the misappropriation of business records described above. Robokoff protests that he only took an employee handbook and was under no duty to return that. But the allegation here is that Robokoff was leading an effort to misappropriate and ultimately control 1st Rate's business records, and that at least presents a question of fact because even if he did not physically or electronically take anything, he nevertheless may have "controlled" the stolen information. Robokoff also argues that even if the Plaintiffs' version of events is believed, his actions never interfered with their right to possess the property because Plaintiffs never lost the actual files and records. The records allegedly stolen were merely copied, not destroyed.

1st Rate argues that when a competitor copies its records, that destroys the value of the records to 1st Rate and interferes with its ability to fully use the information itself. In *Conant v. Karris,* 520 N.E.2d 757 (Ill. App. Ct.1987), the Illinois Court of Appeals allowed a conversion claim to proceed when the defendant allegedly showed another party confidential information but

did not physically give the confidential information to that party. The court found: "Once confidential information is released to competitors, it hardly can be said that the data is still confidential. Thus, the original owner would be deprived of the benefit of the information." 520 N.E.2d at 763. Presumably, the same would hold true under Wisconsin law, and Robokoff has not cited any case even suggesting otherwise. Accordingly, the conversion claim will not be dismissed.

Claim eight alleges that each Defendant was under a contractual duty to keep company information confidential. By disclosing 1st Rate's information to Robokoff's new company, they breached this contractual duty. Robokoff argues that Plaintiffs have not identified the source of this contractual duty, and the Plaintiffs' brief does not elaborate. Plaintiffs insist that there is a factual dispute about the contractual duty, but summary judgment is the "put up or shut up" moment in litigation, *Eberts v. Goderstad,* 569 F.3d 757, 767 (7th Cir. 2009), which means that "the non-moving party is required to marshal and present the court with the evidence she contends will prove her case. And by evidence, we mean evidence on which a reasonable jury could rely." *Goodman v. National Sec. Agency, Inc.,* 621 F.3d 651, 654 (7th Cir. 2010). Because Plaintiffs do not explain what the source of the Defendants' contractual duty is, judgment will be granted to the Defendants on claim eight.

Claim nine alleges misappropriation of trade secrets. Robokoff argues that the information involved – customer lists with accompanying interest rates, debt ratios and credit reports – does not qualify as a trade secret. A trade secret is information that both "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use" and "is the subject of efforts to maintain its secrecy that are reasonable under the circumstances." Wis.

Stat. § 134.90(1)(c). Customer lists are frequently afforded trade secret protection, particularly when they reflect the company's independent compilation and analysis of data. *American Family Mut. Ins. Co. v. Roth,* 485 F.3d 930, 933 (7th Cir. 2007) (noting that "the names in the plaintiff's database are filtered for their suitability to buy insurance, resulting in . . . 'a defined, manageable and economically viable universe of uniquely receptive potential customers.'") That is what we have here. By copying the information from 1st Rate, Robokoff gave himself access to a defined universe of potential customers and would be able to compete for their business by virtue of his knowledge of the interest rates they were paying 1st Rate and their other credit information. It was not just merely a list of customers' identities, but essentially all of the pricing and eligibility data that any other mortgage company would want to know. He protests that his company could have obtained this information from the customers directly, but that is a dubious proposition. Although recent history is littered with identify theft and other financial scams based on such information, most consumers will not willingly divulge their credit information, mortgage interest rate, etc., to a stranger on the telephone. Finally, Robokoff does not argue that 1st Rate failed to treat the data as secret or invested too little effort in developing the information itself. *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.,* 342 F.3d 714, 728-29 n.8 (7th Cir. 2003) (collecting cases). Accordingly, I conclude that claim nine will survive summary judgment.

Finally, claim ten alleges Robokoff committed fraud when he told Plaintiffs that he was leaving the mortgage business entirely and would continue working through the end of his contract in 1st Rate's best interests. Plaintiffs allege they relied on this information to their detriment. They surely would not have let Robokoff continue his employment if they knew the truth about his plans. Plaintiffs allege that the source of Robokoff's duty to tell them the truth was his agreement to return

all records and business information to Plaintiffs. In other words, he essentially promised that he would not lead a conspiracy to steal business information from 1st Rate, and 1st Rate relied on that promise.

But that behavior is the essence of Plaintiffs' breach of contract claim. If one agrees to undertake certain behavior, his failure to do so might be a breach of the contract, but it is not also a fraud. Wisconsin follows the economic loss doctrine. The economic loss doctrine "preclude[es] contracting parties from pursuing tort recovery for purely economic or commercial losses associated with the contract relationship." *Kaloti Enterprises, Inc. v. Kellogg Sales Co.,* 2005 WI 111, 283 Wis.2d 555, 578, 699 N.W.2d 205, 216 (Wis. 2005). Here, the very duty allegedly breached by Robokoff is simply his failure to fulfill the terms of his contract: "Robokoff represented both verbally and in writing (buy-out agreements) that all the plaintiffs' business information would remain the sole property of the plaintiffs and that Robokoff would personally see to the immediate return of any such information." (Pltf. Br. at 28.) Because the fraud claim relies on the same conduct as the breach of contract claim, the economic loss doctrine precludes relief through tort law. (The narrow exception for fraud in the inducement would not apply here. *Kaloti,* 2005 WI 111, 283 Wis. 2d at 585, 699 N.W.2d at 219.) Notably, Robokoff did *not* sign a non-compete agreement, and a fraud claim based on his behavior would essentially create a non-compete where none exists. Accordingly, the Defendants will be granted summary judgment on the fraud claim.[2]

[2]It is hoped that, if this case proceeds to trial, the legal issues can be narrowed down significantly. There does not seem to be an obvious reason to proceed on seven different claims all relying on proof of the same essential conduct.

III. Conclusion

For the reasons given above, the motions for summary judgment are **GRANTED** in part: claims two, eight and ten are **DISMISSED**. The motions are **DENIED** in all other respects.

The clerk is directed to place the case on for a scheduling conference.

SO ORDERED this 14th day of February, 2011.

s/ William C. Griesbach
William C. Griesbach
United States District Judge